




ACCESS POINT DEVICE AND METHOD OF AUTHENTICATION PROCESSING THEREFOR

Patent number: JP2001345819
Publication date: 2001-12-14
Inventor: KIMURA SHINYA
Applicant: SHARP KK
Classification:
 - international: H04L12/28; H04Q7/38; H04L9/32
 - european:
Application number: JP20000164519 20000601
Priority number(s): JP20000164519 20000601

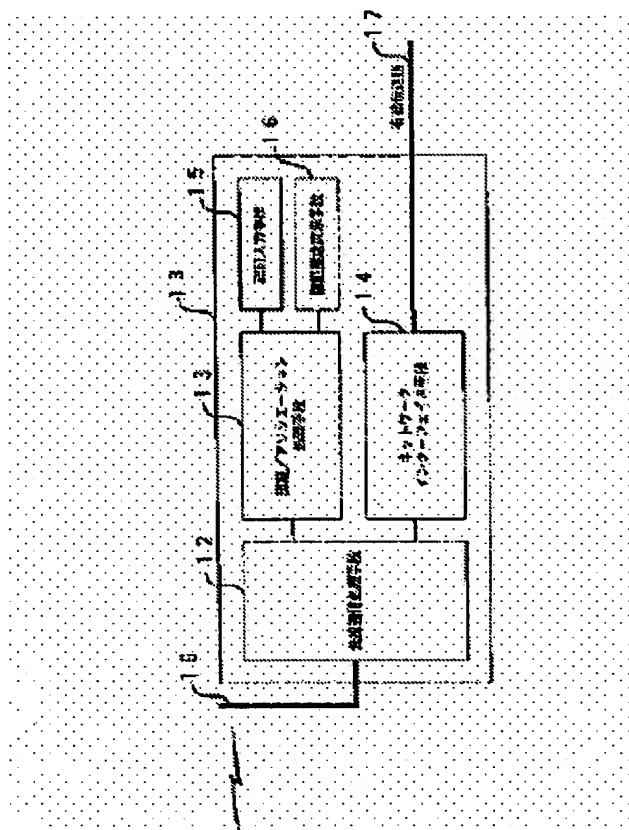
Also published as:

 EP1161031 (A2)
 US2001048744 (A)
 EP1161031 (A3)

Report a data error he

Abstract of JP2001345819

PROBLEM TO BE SOLVED: To provide an access point device and a method of authentication processing therefor, with which a security level can be remarkably improved, in a wireless LAN system. **SOLUTION:** An access point device 18 is provided with an authentication request display means 16 for making the access point device 18 report the existence of a mobile station requesting authentication for obtaining the final permission of an authentication procedure inside an area, to a network manager for managing a LAN, when the mobile station inside the area is to perform the authentication procedure, before the start of an association procedure and an authentication input means 15 for the network manager, who receives the notice, to instruct the permission of refusal of authentication to the mobile station requesting authentication.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-345819

(P2001-345819A)

(43) 公開日 平成13年12月14日 (2001. 12. 14)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テマコード* (参考) |
|---------------------------|-------|---------------|-------------------|
| H 0 4 L | 12/28 | H 0 4 L 11/00 | 3 1 0 B 5 J 1 0 4 |
| H 0 4 Q | 7/38 | H 0 4 B 7/26 | 1 0 9 R 5 K 0 3 3 |
| H 0 4 L | 9/32 | H 0 4 L 9/00 | 6 7 3 A 5 K 0 6 7 |
| | | | 6 7 5 A |

審査請求 未請求 請求項の数 5 O L (全 9 頁)

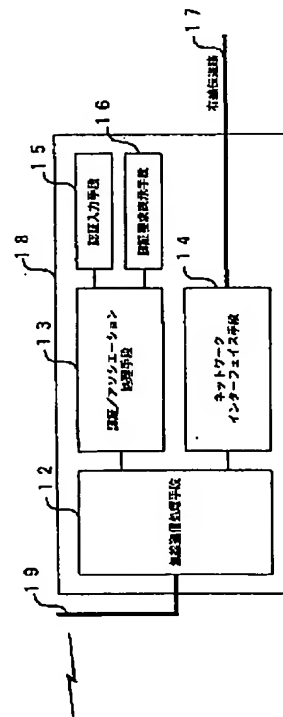
| | | | |
|-----------|------------------------------|----------|--|
| (21) 出願番号 | 特願2000-164519 (P2000-164519) | (71) 出願人 | 000005049 シャープ株式会社 大阪府大阪市阿倍野区長池町22番22号 |
| (22) 出願日 | 平成12年6月1日 (2000. 6. 1) | (72) 発明者 | 木村 真也 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社内 |
| | | (74) 代理人 | 100091096 弁理士 平木 祐輔 |
| | | Fターム(参考) | 5J104 AA07 KA01 KA06 KA10 NA02 5K033 AA08 BA08 DA19 5K067 AA30 DD30 DD51 EE02 EE10 EE22 FF23 HH36 |

(54) 【発明の名称】 アクセスポイント装置及びその認証処理方法

(57) 【要約】

【課題】 ワイヤレスLANシステムにおいて、セキュリティレベルを飛躍的に向上させることができるアクセスポイント装置及びその認証処理方法を提供する。

【解決手段】 アクセスポイント装置18は、エリア内の移動局が、アソシエーション手順を開始する前に認証手順を行う場合に、アクセスポイント装置18が、LANを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がエリア内にいることを通知する認証要求表示手段16と、通知を受けたネットワーク管理者が、認証を求めている移動局に対して認証の許可又は拒否を指示する認証入力手段15とを備える。



(2)

1

【特許請求の範囲】

【請求項1】 有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線LANエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置において、

前記エリア内の移動局が、アソシエーション手順を開始する前に認証手順を行おうとする場合に、前記LANを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がいることを通知する通知手段と、

前記通知を受けた前記ネットワーク管理者による、前記認証を求めている移動局に対しての認証の許可又は拒否の指示が入力される入力手段と、

を備えることを特徴とするアクセスポイント装置。

【請求項2】 有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線LANエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置の認証処理方法において、

前記移動局から前記アクセスポイント装置への認証要求により、前記移動局及び前記アクセスポイント装置が、所定の認証手続を開始する第1ステップと、

前記認証手続により、前記アクセスポイント装置が、前記移動局への認証を許可しようとするとき、前記認証手続における最終メッセージである認証応答メッセージを前記移動局に返信する前に、前記LANを管理するネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートさせる第2ステップと、

前記ネットワーク管理者が、前記アクセスポイント装置に対して、前記認証待ちタイマがタイムアウトする前に、最終の認証の許可又は拒否を指示する第3ステップと、

前記ネットワーク管理者により、前記認証待ちタイマがタイムアウトする前に、最終の認証許可が指示されると、前記アクセスポイント装置が、前記認証応答メッセージを、認証許可として前記移動局に返信する第4ステップと、

前記認証応答メッセージを受信した前記移動局が、アソシエーションの手順を開始する第5ステップと、
 を実行することにより前記移動局の認証が完了し、アソシエーション手順を開始することを特徴とするアクセスポイント装置の認証処理方法。

【請求項3】 前記第3ステップでは、前記ネットワーク管理者が、認証を拒否する指示を前記アクセスポイント装置に指示した場合に、前記認証応答メッセージを、認証拒否として前記移動局に返信することを特徴とする請求項2記載のアクセスポイント装置の認証処理方法。

【請求項4】 前記第3ステップでは、前記ネットワーク管理者が、認証を拒否又は許可する指示を前記アクセ

2

スポイント装置に指示する前に、前記認証待ちタイマがタイムアウトすると、前記認証応答メッセージを、認証拒否として前記移動局に返信することを特徴とする請求項2記載のアクセスポイント装置の認証処理方法。

【請求項5】 前記認証手続は、IEEE 802.11が規定するShared Key Authentication手順であることを特徴とする請求項2乃至4のいずれかに記載のアクセスポイント装置の認証処理方法。

【発明の詳細な説明】

10 【0001】

【発明の属する技術分野】本発明は、アクセスポイント装置及びその認証処理方法に関し、詳細には、無線を利用した、ワイヤレスLANシステムにおいて、悪意を持った侵入者の移動局からの不正なアクセスを防止するためのアクセスポイント装置及びその認証処理方法に関する。

【0002】

【従来の技術】近年、インターネットの爆発的な普及に伴い、オフィス、家庭等で、LAN (Local Area Network) を構築するケースが増えてきている。デジタル無線通信技術の進歩も手伝い、ケーブル配線の煩わしさから、無線でLANを構築する、いわゆるワイヤレスLANのニーズも非常に高まっており、さらに、ノート型パソコンに代表される移動端末での移動環境下における、使用が可能であることも手伝い、将来的には、かなりの数の普及台数が期待されている。このワイヤレスLANの代表的な技術としては、既に、IEEE (Institute of Electrical and Electronics Engineers) において、標準化されている、IEEE 802.11がある。この標準化された技術は、OSIモデルにおける、物理層から、データリンクの下位副層であるMAC (Media Access Control: 媒体アクセス制御) 層までを規定しており、有線のLAN伝送路である、イーサネットと置きかえることができ、さらに、ワイヤレスであるが故の付加機能として、ローミング (roaming) 機能も提供できる仕様になっている。

【0003】さて、有線のイーサネット等で、LANを構築する場合、LANに接続することは、物理的に、ハブ等にケーブルを接続するため、データリンクレベルのセキュリティレベルは非常に高い。つまり、侵入者が、オフィス等に不正に侵入し、端末等をネットワークに接続しようと思っても、ケーブル接続という物理的な作業が必要であり、それを、密に行うことは、一般的なLANの配置状況 (特に、比較的中小規模のLAN) からして、非常に困難である。何故なら、そのLANの利用者と、そのLANを構成するハブやルーター等が、同一の居室内に存在するケースが殆どだからである。一方、ワイヤレスLANシステムの場合は、前記、イーサネット等のケーブル接続の作業は、自動的なアソシエーション (Association) 手順により置き換わる。前

50

(3)

3

記、既存のIEEE 802.11等のシステムにおいて、このアソシエーション手順とは、移動端末が有線等のバックボーン・ネットワークに接続されているアクセスポイントに対して、自分自身の存在を認識してもらうための手順であり、この手順が完了すれば、データ通信を行うことができる。この手順においては、アクセスポイント (access point) のカバーする有限エリアにいる移動端末は、前記アクセスポイントに対して、アソシエーションを行う前に、オプションの認証手続きをすることにより、データリンクレベルのセキュリティを確保することになる。

【0004】このアソシエーション手順によれば、前記移動局は、アソシエーション要求を、前記アクセスポイントに対して行う場合、そのアソシエーション要求メッセージ中に、SSID (Service Set Identifier) を含ませ、これを受信したアクセスポイントは、前記SSIDにて、前記移動局を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、許可する場合は、アソシエーション許可の返信メッセージを、拒否する場合は、アソシエーション拒否の返信メッセージを、前記移動局に送信する。したがって、このアソシエーション手順だけでは、悪意を持ってネットワークに侵入しようとする者が、このSSIDさえ入手してしまえば、簡単にアソシエーションが可能になってしまう。それを避けて、本アソシエーション手順を実行するために、認証手続きを行うオプションが設けられている。つまり、認証手続きを行うオプションを設ける方式によれば、前記移動端末は、本認証手続きを完了しなければ、アソシエーションができないため、データ通信を開始することができず、これは、物理的な接続作業を必要としない、前記有限エリア内の、悪意を持った移動端末からの、不正なアソシエーションを防ぐ有効な機能を提供することになる。

【0005】IEEE 802.11においては、この認証手続きは、Shared Key Authentication手順として定義されており、この手順を図5及び図6により説明する。図5は、従来のワイヤレスLANシステムの概略構成を示す図、図6は、従来の認証手順とアソシエーション手順の制御シーケンスを示す図である。

【0006】図5において、1はワイヤレス・エリア・ネットワーク、2はアクセスポイントAP、3は移動局MT1、4は移動局MT2、5は移動局MT3、6は移動局MT4、7はワイヤレス・エリア・ネットワーク1外の他ネットワークである。

【0007】ある有線伝送路により実現される、他ネットワーク7に接続されたアクセスポイントAP2と、そのアクセスポイントAP2がカバーする、有限なエリアに存在する、移動局MT1、MT2、MT3、MT4から構成されるワイヤレス・エリア・ネットワーク1において、ある移動局 (例えば、MT1) が、電源を投入す

4

るなどの動作により、前記アクセスポイントAP2に対して、アソシエーション前の認証手続きをする場合のシーケンスは、図6に示される。

【0008】まず、移動局MT1は、Shared Key Authentication方法による認証手続きを開始するための、認証要求メッセージ1を、アクセスポイントAP2に送信する。AP認証処理8 (AP認証処理「1」) として、このメッセージを受信したAP2は、この認証手続きの度に、任意に決めることができる、Initialization VectorとSecret Keyの値を、パラメータとし、WEP (Wired Equivalent Privacy) PRNG (Pseudorandom Number Generator) のアルゴリズムに従い数値演算を行い、1280 c t e tの、一意に決まるChallenge Textの値を算出し、この値を含めた認証応答メッセージ1を、移動局MT1に送信する。

【0009】次に、MT認証処理9 (AP認証処理「2」) として、本認証応答メッセージ1を受信した移動局MT1は、その中含まれる前記Challenge Textの値を、WEPの暗号化アルゴリズムに従い、Shared Secret Dataと、Initialization Vectorをパラメータに、暗号化を行い、その値を、前記Initialization Vectorと共に、認証要求メッセージ2に含めて、前記アクセスポイントAP2に返信する。

【0010】さらに、AP認証処理10 (AP認証処理「2」) として、本認証要求メッセージ2を受信した、アクセスポイントAP2は、受信した暗号化されたChallenge Textの値を、同時に受信したInitialization Vectorと、予め知っている前記Shared Secret Dataを基にデコードし、その結果と、前述の元のChallenge Textの値を比較し、それが同一であれば、認証許可とし、同一でなければ、認証拒否とし、その結果を認証応答メッセージ2として、移動局MT1に返信する。そこで、本認証応答メッセージ2を受信した移動局MT1は、その結果が、許可であれば、次のアソシエーションの手順に入ることができ、拒否の場合は、認証失敗ということで、アソシエーション手続きを行うことはできない。

【0011】ここでのアソシエーション処理は、前述の通り、移動局MT1からの、アソシエーション要求メッセージ中の、SSID (Service Set Identifier) を受信したアクセスポイントAP2が、前記SSIDにて、移動局を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、許可する場合は、アソシエーション許可のアソシエーション応答メッセージを、拒否する場合は、アソシエーション拒否のアソシエーション応答メッセージを移動局MT1に送信する。なお、ここでのWEPのアルゴリズムは、RSA Data Security Inc.のRC4技術により規定されている。

【0012】つまり、この認証方法によれば、アクセスポイントと移動局が、あらかじめ、秘密のKeyであるSh

(4)

5

ared Secret Keyを持ち合うことで、アクセスポイントが特定の移動局への認証／アソシエーションを許可する仕組みを実現している。ここで、移動局側は、本Shared Secret Keyを、一般ユーザから、読み取れない実装形態にし、悪意を持った侵入者からの盗難（読み取り）を防ぎ、本Key自体が無線伝送路を行き交うことがないので、傍受されることもなく、ある程度のセキュリティレベルを確保している。

【0013】

【発明が解決しようとする課題】しかしながら、このような従来のアクセスポイント装置の認証処理方法にあつては、認証のためのアルゴリズムと、その認証のためのKeyが、悪意を持ってネットワークに侵入しようとする者に、不正に盗まれないという前提でのセキュリティの確保であり、この前提は100%担保できるものではない。すなわち、正式手順によってアクセスポイントに、認証可能な端末の全クのコピーが、作られないという保証はなく、また、そのユーザからアクセスできないメモリに、格納されているKeyが、特殊な機器を使うことで、不正に読み取られる可能性もないとはいきれない。よって、これらの不正な行為によって、悪意を持ってネットワークに、侵入しようとする者が、ある端末を不正にアソシエーションすることができれば、有線のケーブル接続のような物理的な作業なしに、アクセスポイントのカバーするエリアであれば、物理的に、隠れてネットワークに侵入することができる。つまり、ある閉じられた空間（オフィスや、家庭）内で、ワイヤレスネットワークを構築した場合で、その中心にあるアクセスポイントのカバーするエリア内であれば、その閉じられた区間の外部、つまり、壁等で隔てられた死角にある、悪意を持ってネットワークに侵入しようとする者の端末からのアソシエーションを許してしまう可能性があるという問題があった。

【0014】本発明は、このような課題に鑑みてなされたものであって、ワイヤレスLANシステムにおいて、セキュリティレベルを飛躍的に向上させることができるアクセスポイント装置及びその認証処理方法を提供する。

【0015】

【課題を解決するための手段】本発明のアクセスポイント装置は、有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線LANエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置において、前記エリア内の移動局が、アソシエーション手順を開始する前に認証手順を行おうとする場合に、前記LANを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がいることを通知する通知手段と、前記通知を受けた前記ネットワーク管理者による、前記認証を求めている移動局に対しての認証の許可又は拒否の指示が入力さ

6

れる入力手段と、を備えることを特徴とする。

【0016】本発明のアクセスポイント装置の認証処理方法は、有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線LANエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置の認証処理方法において、前記移動局から前記アクセスポイント装置への認証要求により、前記移動局及び前記アクセスポイント装置が、所定の認証手順を開始する第1ステップと、前記認証手順により、前記アクセスポイント装置が、前記移動局への認証を許可しようとするとき、前記認証手順における最終メッセージである認証応答メッセージを前記移動局に返信する前に、前記LANを管理するネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートさせる第2ステップと、前記ネットワーク管理者が、前記アクセスポイント装置に対して、前記認証待ちタイマがタイムアウトする前に、最終の認証の許可又は拒否を指示する第3ステップと、前記ネットワーク管理者により、前記認証待ちタイマがタイムアウトする前に、最終の認証許可が指示されると、前記アクセスポイント装置が、前記認証応答メッセージを、認証許可として前記移動局に返信する第4ステップと、前記認証応答メッセージを受信した前記移動局が、アソシエーションの手順を開始する第5ステップと、を実行することにより前記移動局の認証が完了し、アソシエーション手順を開始することを特徴とする。

【0017】また、前記第3ステップでは、前記ネットワーク管理者が、認証を拒否する指示を前記アクセスポイント装置に指示した場合に、前記認証手順における最終メッセージである認証応答メッセージを、認証拒否として前記移動局に返信するものであってもよい。

【0018】また、前記第3ステップでは、前記ネットワーク管理者が、認証を拒否又は許可する指示を前記アクセスポイント装置に指示する前に、前記認証待ちタイマがタイムアウトすると、前記認証手順における最終メッセージである認証応答メッセージを、認証拒否として前記移動局に返信するものであってもよい。また、好ましい具体的な態様としては、前記認証手順は、IEEE 802.11が規定するShared Key Authentication手順であってもよい。

【0019】

【発明の実施の形態】以下、添付図面を参照しながら本発明の好適なアクセスポイント装置及びその認証処理方法の実施の形態について詳細に説明する。図1は、本発明の実施の形態のアクセスポイント装置の概略構成を示す図である。

【0020】本実施の形態のアクセスポイント装置18は、前記図5のアクセスポイントAP2に置き換えて設置される。すなわち、前記図5において、ある有線伝送

(5)

7

路により実現される、他ネットワーク7に接続された、アクセスポイントAP2と、そのAP2がカバーする、有限なエリアに存在する移動局MT1、MT2、MT3、MT4から構成される、ワイヤレス・エリア・ネットワーク1において、前記アクセスポイントAP2は、図1に示すアクセスポイント装置18に置き換えて構成される。

【0021】図1において、アクセスポイント装置18は、複数の移動局MT1、MT2、MT3、MT4との無線接続を実現するために、無線変復調部、ベースバンド信号処理部及びデータリンク制御部からなる無線通信処理手段12と、無線通信処理手段12に接続される無線送受信用のアンテナ19と、他ネットワーク7と任意の有線伝送路17によりデータリンク接続し、無線通信処理手段12により送受信されるデータをインターフェースする機能を実現するネットワークインターフェース手段14と、無線通信処理手段12が、複数の移動局とのデータリンク確立を行うためのアソシエーション手順と認証手順を実行し、そこで、必要になる、移動局MT1、MT2、MT3、MT4と交換される制御メッセージを無線通信処理手段12とやりとりする機能を実現する認証／アソシエーション処理手段13と、認証／アソシエーション処理手段13が、認証処理を行う場合に、最終的にそれを許可し、認証許可すべき移動局に認証許可のメッセージを送信する前に、それを通知することで、ワイヤレス・エリア・ネットワーク1を管理するユーザに、表示デバイスやスピーカ等で認証要求している移動局の存在を通知する機能を実現する認証要求表示手段16（通知手段）と、認証要求表示手段16により認証要求している移動局の存在が通知された後に、ワイヤレス・エリア・ネットワーク1を管理するユーザが、それを許可又は拒否することを、認証／アソシエーション処理手段13に通知するためにボタン等の人間の物理的な入力を受け付ける機能を実現する認証入力手段15（入力手段）とから構成される。

【0022】以下、上述のように構成されたアクセスポイント装置の認証処理方法の動作を説明する。ここでは、ある移動局が、電源投入等の動作により、認証処理手順とアソシエーション処理手順が実行され、アクセスポイント装置18とのデータリンク接続が確立される場合と認証が拒否される場合のシーケンスを説明する。

【0023】前記図5における移動局MT1を、認証処理を行う対象の移動局とし、移動局MT2、MT3、MT4は、既にアクセスポイント装置18とアソシエーションまで完了し、データリンクが確立しているものとする。まず、移動局MT1が、認証手続きにより、ネットワークを管理するユーザが、その認証を許可し、その後、アソシエーション手続きにより、アクセスポイント装置18とのデータリンクが確立される場合を、図2及び図4を参照して説明する。

8

【0024】図2は、認証許可の場合の認証手順の制御シーケンスを示す図である。移動局MT1が、電源投入等の動作により、まず、Shared Key Authentication方法による認証手続きを開始するための認証要求メッセージ1をアクセスポイント装置18に送信する。

【0025】アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理1（図2の番号20参照）として、この認証手続きの度に、任意に決めることができる、Initialization VectorとSecret Keyの値をパラメータとし、WEP（Wired Equivalent Privacy）PRNG（Pseudorandom Number Generator）のアルゴリズムに従い数値演算を行い、128ビットの一意に決まるChallenge Textの値を算出し、この値を含めた認証応答メッセージ1を無線通信処理手段12を介して移動局MT1に送信する。

【0026】次に、MT認証処理21として、本認証応答メッセージ1を受信した、移動局MT1は、その中に含まれるChallenge Textの値を、WEPの暗号化アルゴリズムに従い、Shared Secret DataとInitialization Vectorをパラメータにして暗号化を行い、その値をInitialization Vectorと共に、認証要求メッセージ2に含めてアクセスポイント装置18に返信する。さらに、アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理2（図2の番号22参照）として、受信した暗号化されたChallenge Textの値を、同時に受信したInitialization Vectorと予め知っているShared Secret Dataを基にデコードし、その結果と前述の元のChallenge Textの値を比較し、それが同一であれば、AP認証処理3（図2の番号23参照）の手順を実行する。この手順を示したのが図4に示すフローのステップS30～ステップS33の処理である。

【0027】図4は、上記アクセスポイントの認証処理を示すフローチャートである。まず、この手順においては、アクセスポイント装置18の認証／アソシエーション処理手順13は、認証要求表示手段16に対して、認証待ちであることを通知し（ステップS30）、それと同時に、任意の時間に設定された認証待ちタイマをスタートさせ（ステップS31）、認証入力待ち（ステップS32）の状態に入る。一方、認証待ちであることの通知を受けた、認証要求表示手段16は、直ぐに、ネットワークを管理するユーザに対して表示デバイスやスピーカ等で認証要求している移動局が存在することを通知する。

【0028】ここで、認証／アソシエーション処理手順13は、認証待ちタイマがタイムアウトする前に認証入力手段16からのネットワークを管理するユーザの認証許可の入力による認証許可入力の通知を受ければ、認証許可を示した認証応答メッセージ2を無線通信処理手段

(6)

9

12を介して移動局MT1に送信する（ステップS33）。

【0029】図2に戻って、本認証応答メッセージ2を受信した移動局MT1は、その結果が、許可であることから、次のアソシエーションの手順に入り、アソシエーション要求メッセージを、アクセスポイント装置18へ送信する。

【0030】ここで、アクセスポイント装置18においては、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、アソシエーション処理（図2の番号24参照）として、アソシエーション要求メッセージ中のSSID（Service Set Identifier）にて、移動局MT1を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、それを許可するときは、無線通信処理手段12を介して移動局MT1へアソシエーション許可を示したアソシエーション応答メッセージを送信する。このアソシエーション応答メッセージを移動局MT1が受信すれば、移動局MT1とアクセスポイント装置18の間でデータリンクが確立され、以降、データの通信が可能になる。

【0031】次に、移動局MT1が、認証手続きにおいて、ネットワークを管理するユーザにより、その認証を拒否される場合、及び、認証待ちタイマがタイムアウトして、自動的に、認証が拒否される場合を図3及び図4を参照して説明する。

【0032】図3は、認証拒否／タイムアウト場合の認証手順の制御シーケンスを示す図である。図3において、移動局MT1が、電源投入等の動作により、Shared Key Authentication方法による認証手続きを開始するための認証要求メッセージ1をアクセスポイント装置18に送信する。

【0033】アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理1（図3の番号25参照）としてこの認証手続きの度に、任意に決めることができる、Initialization VectorとSecret Keyの値をパラメータとし、WEP（Wired Equivalent Privacy）PRNG（Pseudorandom Number Generator）のアルゴリズムに従い数値演算を行い、1280c t e tの一意に決まるChallenge Textの値を算出し、この値を含めた認証応答メッセージ1を、無線通信処理手段12を介して、移動局MT1に送信する。

【0034】次に、MT認証処理（図3の番号26参照）として、本認証応答メッセージ1を受信した移動局MT1は、その中含まれるChallenge Textの値を、WEPの暗号化アルゴリズムに従い、Shared Secret Dataと、Initialization Vectorをパラメータに暗号化を行い、その値をInitialization Vectorと共に、認証要求メッセージ2に含めてアクセスポイント装置18に返信

10

する。さらに、アクセスポイント装置18において、無線通信処理手段12を介して、このメッセージを受信した認証／アソシエーション処理手段13は、AP認証処理2（図3の番号27参照）として受信した暗号化されたChallenge Textの値を、同時に受信したInitialization Vectorと予め知っているShared Secret Dataを基にデコードし、その結果と前述の元のChallenge Textの値を比較し、それが同一であればAP認証処理3（図3の番号28参照）の手順を実行する。この手順を示したのが図4に示すフローのステップS30～ステップS32、ステップS34の処理である。

【0035】まず、この手順においては、アクセスポイント装置18の認証／アソシエーション処理手順13は、認証要求表示手段16に対して認証待ちであることを通知し（ステップS30）、それと同時に、任意の時間に設定された認証待ちタイマをスタートさせ（ステップS31）、認証入力待ち（ステップS32）の状態に入る。一方、認証待ちであることの通知を受けた認証要求表示手段16は、直ぐに、ネットワークを管理するユーザに対して表示デバイスやスピーカ等で認証要求している移動局が存在することを通知する。

【0036】ここで、認証／アソシエーション処理手順13は、認証待ちタイマがタイムアウトする前に認証入力手段16からのネットワークを管理するユーザの認証拒否の入力による認証拒否入力の通知を受ければ、認証拒否を示した認証応答メッセージ2を無線通信処理手段12を介して移動局MT1に送信する（ステップS34）。同様に、認証入力待ち（ステップS32）の状態において、認証待ちタイマがタイムアウトすれば、認証拒否を示した認証応答メッセージ2を無線通信処理手段12を介して移動局MT1に送信する（ステップS34）。

【0037】図3に戻って、本認証応答メッセージ2を受信した移動局MT1は、その結果が拒否であることから次のアソシエーションの手順には入れず、必要があれば、ユーザに対して認証が失敗したことを通知する（図3の番号29参照）。よって、この場合は、移動局MT1は、データ通信を行うことができない。

【0038】なお、ここで言及している、WEPのアルゴリズムは、RSA Data Security Inc.のRC4技術により規定されており、また、アソシエーション処理（図2の番号24参照）も、IEEE802.11で規定されるアソシエーション手順と同一であることとする。

【0039】また、ここでの認証待ちタイマに設定されている任意の時間とは、ネットワークを管理するユーザが、認証要求表示手段により、認証待ちの移動局が存在することを認識してから、それを許可するために、認証入力手段により、許可の入力をするまでに必要な時間から換算される妥当な値として、ネットワークを管理するユーザが、任意に設定可能であるものとする。

(7)

11

【0040】以上述べたように、本実施の形態では、アクセスポイント装置18は、エリア内の移動局が、アソシエーション手順を開始する前に認証手順を行う場合に、アクセスポイント装置18が、LANを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がエリア内にいることを通知する認証要求表示手段16と、通知を受けたネットワーク管理者が、認証を求めている移動局に対して認証の許可又は拒否を指示する認証入力手段15とを備え、物理的に目視できないがために、悪意を持った、ネットワークへの侵入者の攻撃を受けやすい、ワイヤレスLANシステムにおいて、移動局のアソシエーション前の認証手続きで、アクセスポイントがそれを許可することを自動的に行わず、そのネットワークを管理するユーザが、誰がアソシエーションしようとしているのかを目視した上で、その許可を与えることができるので、セキュリティレベルを飛躍的に向上させることができる。

【0041】また、この認証の手順は、IEEE802.11で、オプションとして規定されている、Shared Key Authentication手順を実装しているワイヤレスLANシステムにおいては、アクセスポイント装置についてのみ追加の実装が必要であり、移動局装置は、なんら変更をすることなく機能させることが可能である。

【0042】

【発明の効果】以上、詳述したように、本発明によれば、ワイヤレスLANシステムにおいて、セキュリティレベルを飛躍的に向上させることができ、また、移動局装置は、なんら変更をすることなく実施することができる。

【図面の簡単な説明】

12

【図1】本発明の実施の形態のアクセスポイント装置の概略構成を示す図である。

【図2】本実施の形態のアクセスポイント装置の認証許可の場合の認証手順の制御シーケンスを示す図である。

【図3】本実施の形態のアクセスポイント装置の認証拒否/タイムアウト場合の認証手順の制御シーケンスを示す図である。

【図4】本実施の形態のアクセスポイント装置のアクセスポイントの認証処理を示すフローチャートである。

【図5】従来のワイヤレスLANシステムの概略構成を示す図である。

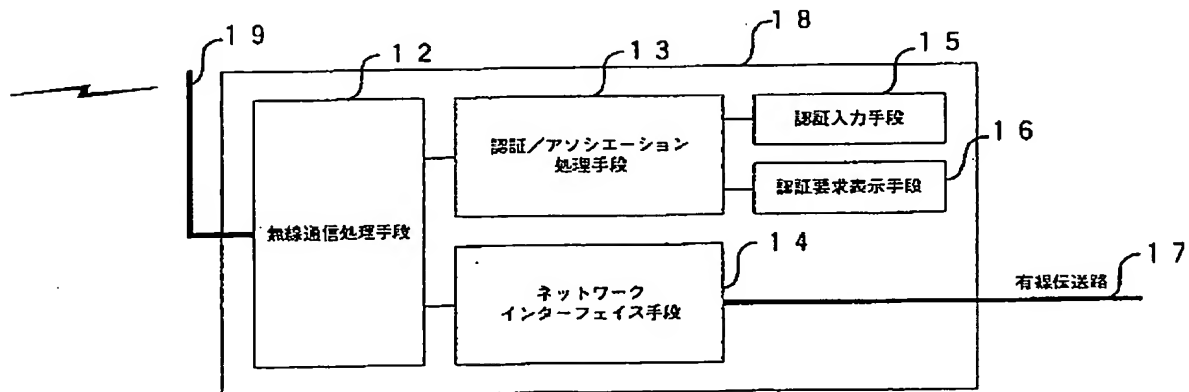
【図6】従来のワイヤレスLANシステムの認証手順とアソシエーション手順の制御シーケンスを示す図である。

【符号の説明】

- 1 ワイヤレス・エリア・ネットワーク
- 3 移動局MT 1
- 4 移動局MT 2
- 5 移動局MT 3
- 6 移動局MT 4
- 7 他ネットワーク
- 12 無線通信処理手段
- 13 認証/アソシエーション処理手段
- 14 ネットワークインターフェース手段
- 15 認証入力手段（入力手段）
- 16 認証要求表示手段（通知手段）
- 17 有線伝送路
- 18 アクセスポイント装置
- 19 無線送受信用のアンテナ

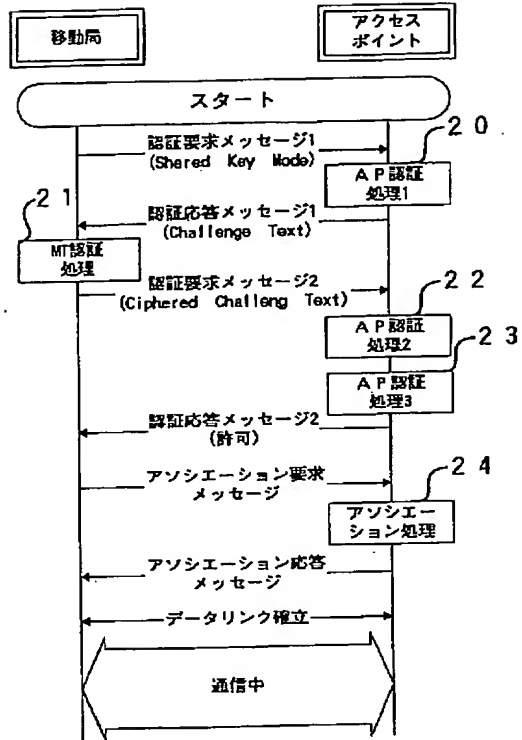
30

【図1】

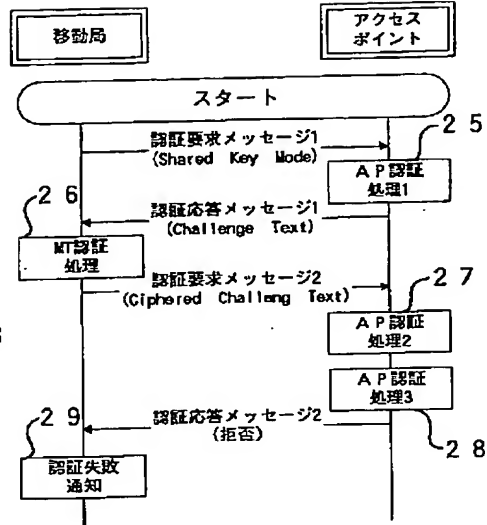


(8)

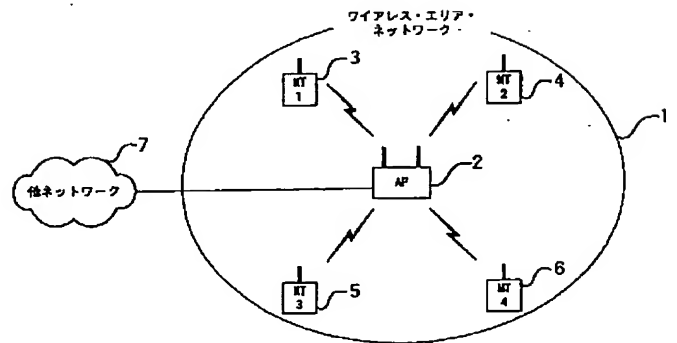
【図2】



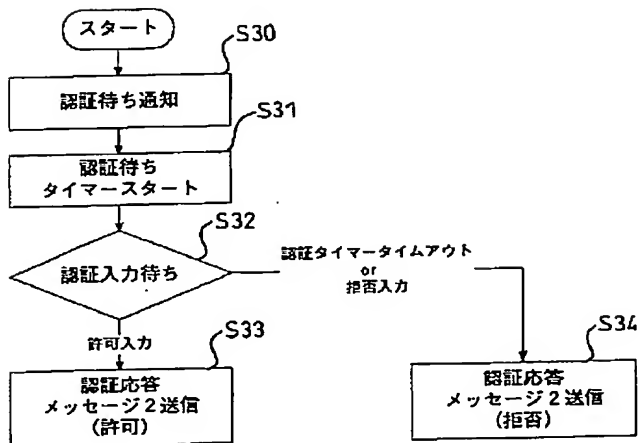
【図3】



【図5】

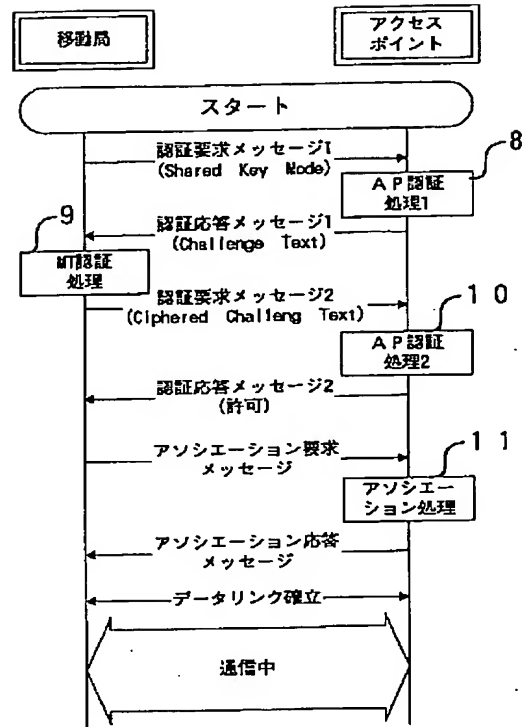


【図4】



(9)

【図 6】



* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the access point equipment which is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area When the mobile station in said area tends to perform an authentication procedure before starting an association procedure, in order to obtain final authorization of an authentication procedure to the network administrator who manages said LAN Access point equipment characterized by having an input means by which authorization of the authentication over the mobile station which is searching for said authentication by notice means to notify that the mobile station which is searching for authentication is, and said network administrator who received said notice, or directions of refusal is inputted.

[Claim 2] In the authentication art of access point equipment which is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area From said mobile station in the 1st step to which said mobile station and said access point equipment start a predetermined authentication procedure by the authentication demand of said access point equipment HE, and said authentication procedure When said access point equipment tends to permit the authentication to said mobile station, Before answering said mobile station in the authentication response message which is the last message in said authentication procedure, while notifying final authorization of said authentication procedure to the network administrator who manages said LAN The 2nd step which starts the waiting timer for authentication which set up the maximum latency time until the last authentication is performed, Before said waiting timer for authentication carries out a time-out to said access point equipment, said network administrator by the 3rd step which directs authorization or refusal of last of authentication, and said network administrator If the last authentication authorization is directed before said waiting timer for authentication carries out a time-out The 4th step as which said access point equipment answers said mobile station considering said authentication response message as authentication authorization, The authentication art of the access point equipment characterized by completing authentication of said mobile station and starting an association procedure by performing the 5th step to which said mobile station which received said authentication response message starts the procedure of an association.

[Claim 3] The authentication art of the access point equipment according to claim 2 characterized by answering said mobile station considering said authentication response message as authentication refusal when said network administrator directs the directions which refuse authentication to said access point equipment at said 3rd step.

[Claim 4] The authentication art of the access point equipment according to claim 2 which will be characterized by answering said mobile station considering said authentication response message as authentication refusal if said waiting timer for authentication carries out a time-out before said network administrator directs the directions with which authentication is refused or permitted to said access point equipment at said 3rd step.

[Claim 5] Said authentication procedure is the authentication art of the access point equipment according

to claim 2 to 4 characterized by being the Shared Key Authentication procedure which IEEE802.11 specifies.

[Translation done.]

* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the access point equipment and its authentication art for preventing unjust access from the mobile station of the invader who had malice in the detail in the wireless LAN system using wireless about access point equipment and its authentication art.

[0002]

[Description of the Prior Art] In recent years, the cases where LAN (Local Area Network) is built at office, a home, etc. have been increasing in number with the explosive spread of the Internet. The advance of digital radio communication technology is also helped, from the troublesomeness of cable wiring, the needs of the so-called wireless LAN which build LAN by wireless are also increasing very much, further, it helps for the use under the migration environment in the migration terminal represented by the notebook sized personal computer to be also possible, and most number of number of spread is expected in the future. As a typical technique of this wireless LAN, there is already IEEE802.11 standardized in IEEE (Institute of Electrical and Electronics Engineers). This standardized technique has specified from the physical layer to the MAC (Media Access Control: media access control) layer in an OSI model which is a low order sublayer of a data link, can replace it with Ethernet which is the LAN transmission line of a cable, and further, although it is wireless, it is the specification which can also offer a roaming (roaming) function as an addition function of a reason.

[0003] Now, when building LAN with Ethernet of a cable etc., in order that connecting with LAN may connect a cable to a hub etc. physically, the security level of data link level is very high. That is, even if an invader trespasses upon office etc. unjustly and regards a terminal etc. as it connecting with a network, the physical activity of cable splicing is required, and it is very difficult [it] to perform it secretly, considering the arrangement situation (especially comparatively LAN of a minor scale) of general LAN. It is because the case where a hub, a router, etc. which constitute the LAN with the user of the LAN exist in the same sitting-room is most. On the other hand, in the case of a wireless LAN system, the activity of cable splicing, such as the above and Ethernet, replaces with an automatic association (Association) procedure. In systems, such as the above and existing IEEE802.11, this association procedure is a procedure for having one's existence recognized to the access point where the migration terminal is connected to backbone networks, such as a cable, and if this procedure is completed, data communication can be performed. In this procedure, the migration terminal which is present in the finite area which an access point (access point) covers will secure the security of data link level by carrying out authentication procedure of an option, before performing an association to said access point.

[0004] According to this association procedure, said mobile station When an association demand is given to said access point, The access point which was made to contain SSID (Service Set Identifier) in the association demand message, and received this In said SSID, identify said mobile station, determine whether permit the association according to the association authorization Ruhr decided beforehand, and when granting a permission When refusing the reply message of association authorization, the reply

message of association refusal is transmitted to said mobile station. Therefore, only in this association procedure, if those who are going to have malice and are going to trespass upon a network receive even this SSID, an association will become possible simply. In order to avoid it and to perform this association procedure, the option which performs authentication procedure is formed. That is, if said migration terminal does not complete this authentication procedure, since an association cannot do it according to the method which forms the option which performs authentication procedure, data communication cannot be started but this will offer the effective function which prevents the unjust association from the migration terminal with the malice in said finite area which does not need physical connection.

[0005] In IEEE802.11, this authentication procedure is defined as a Shared Key Authentication procedure, and explains this procedure by drawing 5 and drawing 6. Drawing in which drawing 5 shows the outline configuration of the conventional wireless LAN system, and drawing 6 are drawings showing the control sequence of the conventional authentication procedure and an association procedure.

[0006] drawing 5 -- setting -- 1 -- for a mobile station 1 and MT 4, a mobile station 2 and MT 5 is [a wireless area network and 2 / an access point AP and 3 / the mobile stations 4 and MT 7 of a mobile station 3 and MT 6] the other networks outside the wireless area network 1.

[0007] The access point AP 2 which is realized by a certain cable-transmission way and which was connected to the other networks 7 In the wireless area network 1 which the access point AP 2 covers, which exists in limited area and which consists of mobile stations MT1, MT2, MT3, and MT4 A sequence in case a certain mobile station (for example, MT1) carries out authentication procedure before an association to said access point AP 2 by actuation of switching on a power source is shown in drawing 6.

[0008] First, a mobile station MT 1 transmits the authentication demand message 1 for starting the authentication procedure by the Shared Key Authentication approach to an access point AP 2. AP2 which received this message as AP authentication processing 8 (AP authentication processing "1") The value of Initialization Vector and Secret Key which can be decided at every authentication procedure of this at arbitration Consider as a parameter and math processing is performed according to the algorithm of WEP(Wired Equivalent Privacy) PRNG (Pseudorandom Number Generator). The value of Challenge Text it is decided that will be the meaning of 1280ctet(s) is computed, and the authentication response message 1 including this value is transmitted to a mobile station MT 1.

[0009] Next, as MT authentication processing 9 (AP authentication processing "2"), the mobile station MT 1 which received this authentication response message 1 enciphers Initialization Vector in a parameter with Shared Secret Data in the value of said Challenge Text contained the inside according to the encryption algorithm of WEP, includes the value in the authentication demand message 2 with said Initialization Vector, and answers said access point AP 2.

[0010] Furthermore, the access point AP 2 which received this authentication demand message 2 as AP authentication processing 10 (AP authentication processing "2") Initialization Vector which received the value of enciphered Challenge Text which received to coincidence, Decode based on said Shared Secret Data known beforehand, compare the result with the value of Challenge Text of the origin of the above-mentioned, and if it is the same It considers as authentication authorization, and if not the same, it will consider as authentication refusal and a mobile station MT 1 will be answered by making the result into the authentication response message 2. Then, if the result is authorization, the mobile station MT 1 which received this authentication response message 2 can go into the procedure of the next association, when it is refusal, it is authentication failure, and cannot perform association procedure.

[0011] When the access point AP 2 which received SSID (Service Set Identifier) in the association demand message from a mobile station MT 1 identifies a mobile station in said SSID, and determines whether permit the association according to the association authorization Ruhr decided beforehand, it grants a permission as above-mentioned and association processing here refuses the association response message of association authorization, it transmits the association response message of association refusal to a mobile station MT 1. In addition, the algorithm here of WEP is prescribed by RC4 technique of RSA Data Security Inc.

[0012] that is, -- according to this authentication approach -- an access point and a mobile station -- oh, the structure which an access point permits the authentication/association to a specific mobile station is realized by sharing eye ** and each other's Shared Secret Key which is secret Key. Here, a certain amount of security level is secured, without being monitored, since it is made the mounting gestalt which cannot read Book Shared Secret Key in a general user, a mobile station side prevents the theft (reading) from an invader with malice and this Key itself does not go a radio-transmission way back and forth.

[0013]

[Problem(s) to be Solved by the Invention] However, if it is in the authentication art of such conventional access point equipment, it is reservation of the security in the premise of not being unjustly stolen by those by whom the algorithm for authentication and Key for that authentication tend to have malice, and tend to trespass upon a network, and this premise cannot be collateralized 100%. That is, it is that Key stored in the memory in which no guarantee that the entire copy of the terminal which can be attested to an access point is not made is and, which cannot be accessed from the user by the formal procedure uses a special device, and cannot declare that it must have been read unjustly. Therefore, if those who are going to have malice and are going to trespass upon a network by these unjust actions are the area which an access point covers without a physical activity like the cable splicing of a cable if the association of a certain terminal can be carried out unjustly, physically, they can hide and can trespass upon a network. That is, there was a problem which is in the dead angle separated by the exterior of the closed section, i.e., a wall etc., if it is in the area which the access point which exists at the core covers by the case where a wireless network is built that the association from the terminal of those who are going to trespass upon a network with malice might be allowed, in a certain closed space (office and home).

[0014] This invention is made in view of such a technical problem, and offers the access point equipment which can raise security level by leaps and bounds, and its authentication art in a wireless LAN system.

[0015]

[Means for Solving the Problem] In the access point equipment which the access point equipment of this invention is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area When the mobile station in said area tends to perform an authentication procedure before starting an association procedure, in order to obtain final authorization of an authentication procedure to the network administrator who manages said LAN It is characterized by having an input means by which authorization of the authentication over the mobile station which is searching for said authentication by notice means to notify that the mobile station which is searching for authentication is, and said network administrator who received said notice, or directions of refusal is inputted.

[0016] The authentication art of the access point equipment of this invention In the authentication art of access point equipment which is equipped with an interface function with the network built on a cable-transmission way, and makes data link connection with two or more mobile stations in wireless LAN area From said mobile station in the 1st step to which said mobile station and said access point equipment start a predetermined authentication procedure by the authentication demand of said access point equipment HE, and said authentication procedure When said access point equipment tends to permit the authentication to said mobile station, Before answering said mobile station in the authentication response message which is the last message in said authentication procedure, while notifying final authorization of said authentication procedure to the network administrator who manages said LAN The 2nd step which starts the waiting timer for authentication which set up the maximum latency time until the last authentication is performed, Before said waiting timer for authentication carries out a time-out to said access point equipment, said network administrator by the 3rd step which directs authorization or refusal of last of authentication, and said network administrator If the last authentication authorization is directed before said waiting timer for authentication carries out a time-out The 4th step as which said access point equipment answers said mobile station considering said

authentication response message as authentication authorization, By performing the 5th step to which said mobile station which received said authentication response message starts the procedure of an association, authentication of said mobile station is completed and it is characterized by starting an association procedure.

[0017] Moreover, at said 3rd step, when said network administrator directs the directions which refuse authentication to said access point equipment, said mobile station may be answered considering the authentication response message which is the last message in said authentication procedure as authentication refusal.

[0018] Moreover, at said 3rd step, if said waiting timer for authentication carries out a time-out before said network administrator directs the directions with which authentication is refused or permitted to said access point equipment, said mobile station may be answered considering the authentication response message which is the last message in said authentication procedure as authentication refusal. Moreover, as a desirable concrete mode, said authentication procedure may be a Shared Key Authentication procedure which IEEE802.11 specifies.

[0019]

[Embodiment of the Invention] Hereafter, the gestalt of operation of the suitable access point equipment of this invention and its authentication art is explained to a detail, referring to an accompanying drawing. Drawing 1 is drawing showing the outline configuration of the access point equipment of the gestalt of operation of this invention.

[0020] The access point equipment 18 of the gestalt of this operation is replaced and installed in the access point AP 2 of said drawing 5 . That is, in said drawing 5 , in the access point AP 2 which is realized by a certain cable-transmission way and which was connected to the other networks 7, and the wireless area network 1 which the AP2 covers and which consists of mobile stations MT1, MT2, MT3, and MT4 which exist in limited area, said access point AP 2 is transposed to the access point equipment 18 shown in drawing 1 , and is constituted.

[0021] In drawing 1 access point equipment 18 In order to make wireless connection with two or more mobile stations MT1, MT2, MT3, and MT4 The radio processing means 12 which consists of the wireless strange recovery section, the baseband signaling processing section, and the data-link-control section, The antenna 19 for wireless transmission and reception connected to the radio processing means 12, A network interface means 14 to realize the function which interfaces the data which make data link connection by the other networks 7 and the cable-transmission way 17 of arbitration, and are transmitted and received by the radio processing means 12, The radio processing means 12 performs the association procedure and authentication procedure for performing data link establishment with two or more mobile stations. There Needed authentication / association processing means 13 to realize the function to exchange with the radio processing means 12 the control message exchanged for mobile stations MT1, MT2, MT3, and MT4, When authentication / association processing means 13 performs authentication processing, before permitting it finally and transmitting the message of authentication authorization to the mobile station which should carry out authentication authorization, by notifying it An authentication demand display means 16 (notice means) to realize the function which notifies the user who manages the wireless area network 1 of the existence of a mobile station which is carrying out the authentication demand by the display device, the loudspeaker, etc., After the existence of a mobile station which is carrying out the authentication demand with the authentication demand display means 16 is notified In order that the user who manages the wireless area network 1 may notify permitting or refusing it to authentication / association processing means 13, it consists of authentication input means 15 (input means) to realize the function to receive the physical input of human beings, such as a carbon button.

[0022] Hereafter, actuation of the authentication art of the access point equipment constituted as mentioned above is explained. Here, authentication procedure and association procedure are performed for a certain mobile station by powering on's etc. actuation, and a sequence in case the case where the data link connection with access point equipment 18 is established, and authentication are refused is explained.

[0023] The mobile station MT 1 in said drawing 5 should be used as the mobile station of the object

which performs authentication processing, mobile stations MT2, MT3, and MT4 should already be completed to access point equipment 18 and an association, and the data link shall be established. First, the user to whom a mobile station MT 1 manages a network in authentication procedure permits the authentication, and association procedure explains after that the case where a data link with access point equipment 18 is established, with reference to drawing 2 and drawing 4 .

[0024] Drawing 2 is drawing showing the control sequence of the authentication procedure in authentication authorization. A mobile station MT 1 transmits the authentication demand message 1 for starting the authentication procedure by the Shared Key Authentication approach to access point equipment 18 first by powering on's etc. actuation.

[0025] In access point equipment 18, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As AP authentication processing 1 (number 20 reference of drawing 2), at every authentication procedure of this The value of Initialization Vector and Secret Key which can be decided to be arbitration is made into a parameter. Math processing is performed according to the algorithm of WEP(WiredEquivalent Privacy) PRNG (Pseudorandom Number Generator). The value of Challenge Text it is decided that will be the meaning of 1280tet(s) is computed, and the authentication response message 1 including this value is transmitted to a mobile station MT 1 through the radio processing means 12.

[0026] Next, as MT authentication processing 21, the mobile station MT 1 which received this authentication response message 1 enciphers the value of Challenge Text contained in it by making Shared Secret Data and Initialization Vector into a parameter according to the encryption algorithm of WEP, includes the value in the authentication demand message 2 with Initialization Vector, and answers access point equipment 18. In access point equipment 18, furthermore, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As AP authentication processing 2 (number 22 reference of drawing 2), the value of enciphered Challenge Text which received It decodes based on Initialization Vector which received to coincidence, and Shared Secret Data known beforehand. The result is compared with the value of above-mentioned original Challenge Text, and if it is the same, the procedure of AP authentication processing 3 (number 23 reference of drawing 2) will be performed. Processing of step S30 of the flow shown in drawing 4 - step S33 showed this procedure.

[0027] Drawing 4 is a flow chart which shows authentication processing of the above-mentioned access point. first, in this procedure, to the authentication demand display means 16, authentication / association procedure 13 of access point equipment 18 notify that it is the waiting for authentication (step S30), starts it, simultaneously the waiting timer for authentication set as the time amount of arbitration (step S31), and goes into the condition of the waiting for an authentication input (step S32). An authentication demand display means 16 by which the notice of being the waiting for authentication was received on the other hand notifies that the mobile station which is carrying out the authentication demand by the display device, the loudspeaker, etc. immediately to the user who manages a network exists.

[0028] Here, if the notice of the authentication authorization input by the input of the user who manages the network from the authentication input means 16 of authentication authorization is received before the waiting timer for authentication carries out the time-out of authentication / the association procedure 13, the authentication response message 2 which showed authentication authorization will be transmitted to a mobile station MT 1 through the radio processing means 12 (step S33).

[0029] It returns to drawing 2 , and since the result is authorization, the mobile station MT 1 which received this authentication response message 2 goes into the procedure of the next association, and transmits an association demand message to access point equipment 18.

[0030] It sets to access point equipment 18 here. Authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As association processing (number 24 reference of drawing 2), in SSID in an association demand message (Service Set Identifier) When identifying a mobile station MT 1, determining whether permit the association according to the association authorization Ruhr decided beforehand and permitting it The association response message

which showed association authorization to the mobile station MT 1 through the radio processing means 12 is transmitted. If a mobile station MT 1 receives this association response message, a data link will be established between a mobile station MT 1 and access point equipment 18, and the communication link of data will be attained henceforth.

[0031] Next, when a mobile station MT 1 has the authentication refused by the user who manages a network in authentication procedure, the waiting timer for authentication carries out a time-out, and the case where authentication is refused is automatically explained with reference to drawing 3 and drawing 4.

[0032] Drawing 3 is drawing showing the control sequence of the authentication procedure of authentication refusal / time-out case. In drawing 3, a mobile station MT 1 transmits the authentication demand message 1 for starting the authentication procedure by the Shared Key Authentication approach to access point equipment 18 by powering on's etc. actuation.

[0033] In access point equipment 18, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 As AP authentication processing 1 (number 25 reference of drawing 3), at every authentication procedure of this The value of Initialization Vector and Secret Key which can be decided to be arbitration is made into a parameter. Math processing is performed according to the algorithm of WEP(Wired Equivalent Privacy) PRNG (Pseudorandom Number Generator). The value of Challenge Text it is decided that will be the meaning of 1280ctet(s) is computed, and the authentication response message 1 including this value is transmitted to a mobile station MT 1 through the radio processing means 12.

[0034] Next, as MT authentication processing (number 26 reference of drawing 3), the mobile station MT 1 which received this authentication response message 1 enciphers Initialization Vector as Shared Secret Data in a parameter in the value of Challenge Text contained the inside according to the encryption algorithm of WEP, includes the value in the authentication demand message 2 with Initialization Vector, and answers access point equipment 18. In access point equipment 18, furthermore, authentication / an association processing means 13 by which this message was received, through the radio processing means 12 The value of enciphered Challenge Text which received as AP authentication processing 2 (number 27 reference of drawing 3) It decodes based on Initialization Vector which received to coincidence, and Shared Secret Data known beforehand. The result is compared with the value of above-mentioned original Challenge Text, and if it is the same, the procedure of AP authentication processing 3 (number 28 reference of drawing 3) will be performed. Processing of step S30 of the flow shown in drawing 4 - step S32, and step S34 showed this procedure.

[0035] first, in this procedure, authentication / association procedure 13 of access point equipment 18 notify that it is the waiting for authentication to the authentication demand display means 16 (step S30), starts it, simultaneously the waiting timer for authentication set as the time amount of arbitration (step S31), and goes into the condition of the waiting for an authentication input (step S32). An authentication demand display means 16 by which the notice of being the waiting for authentication was received on the other hand notifies that the mobile station which is carrying out the authentication demand by the display device, the loudspeaker, etc. immediately to the user who manages a network exists.

[0036] Here, if the notice of the authentication refusal input by the input of the user who manages the network from the authentication input means 16 of authentication refusal is received before the waiting timer for authentication carries out the time-out of authentication / the association procedure 13, the authentication response message 2 which showed authentication refusal will be transmitted to a mobile station MT 1 through the radio processing means 12 (step S34). Similarly, if the waiting timer for authentication carries out a time-out in the condition of the waiting for an authentication input (step S32), the authentication response message 2 which showed authentication refusal will be transmitted to a mobile station MT 1 through the radio processing means 12 (step S34).

[0037] If it returns to drawing 3, the mobile station MT 1 which received this authentication response message 2 is not put into the procedure of the next association since the result is refusal, but there is need, what authentication went wrong to the user will be notified (number 29 reference of drawing 3 R> 3). Therefore, a mobile station MT 1 cannot perform data communication in this case.

[0038] In addition, the algorithm of WEP which has made reference here is made the same as that of the association procedure in which it is prescribed by RC4 technique of RSA Data Security Inc., and association processing (number 24 reference of drawing 2 R> 2) is also specified by IEEE802.11.

[0039] Moreover, after the user who manages a network recognizes it that the mobile station of the waiting for authentication exists to be the time amount of the arbitration set as the waiting timer for authentication here with an authentication demand display means, in order to permit it, the user who manages a network considers as what can be set as arbitration as an appropriate value which will be converted from required time amount by the authentication input means by the time it inputs authorization.

[0040] As stated above, with the gestalt of this operation access point equipment 18 When the mobile station in area performs an authentication procedure before starting an association procedure, in order that access point equipment 18 may obtain final authorization of an authentication procedure to the network administrator who manages LAN An authentication demand display means 16 to notify that the mobile station which is searching for authentication is in area, To eye backlash which it has an authentication input means 15 by which the network administrator who received the notice directs authorization or refusal of authentication to the mobile station which is searching for authentication, and cannot be viewed physically In the wireless LAN system with malice which is easy to receive an attack of the invader of network WAKUHE in the authentication procedure before the association of a mobile station It does not perform automatically that an access point permits it, but after who views whether it is going to carry out the association, since the user who manages the network can give the authorization, he can raise security level by leaps and bounds.

[0041] Moreover, the procedure of this authentication is IEEE802.11, in the wireless LAN system which is specified as an option and which mounts the Shared Key Authentication procedure, additional mounting is required only about access point equipment, and, as for mobile station equipment, it is possible to make it function, without changing in any way.

[0042]

[Effect of the Invention] As mentioned above, according to this invention, as explained in full detail, in a wireless LAN system, security level can be raised by leaps and bounds, and mobile station equipment can be carried out, without changing in any way.

[Translation done.]